Alliance LogAgent for IBM i
Performance Tuning Tech Notes

Alliance LogAgent for IBM i and Application Performance

Many things can affect the performance of the Alliance LogAgent application. This document provides some guidance and suggestions on how you can get the best performance in your environment.

High Speed Event Management

Poor performance can consume CPU resources and slow event management, defeating your security strategy. On an entry level IBM i platform, Alliance LogAgent processed over 3,500 events per second with minimal impact on CPU.

Townsend SECURITY

Meet Compliance Regulations
Collect security system logs and transmit to a log collection server

Formats QAUDJRN Security Journal
Format to syslog (RFC3164) or Common Event Format (CEF)

Communicates Securely
Communicates with log collection servers and Security Information & Event Management (SIEM) solutions

High Performance
Event management protects CPU resources with high event processing speeds

Affordable Solution
Protects your investment in IBM i hardware and software

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360.357.9047

System Audit Event Configuration

System Values

The primary cause of performance problems with security event collection arises when the IBM i is configured to collect the maximum number of security events in the QAUDJRN security journal. The type of events that the system will collect in this journal is controlled by the system values QAUDLVL and QAUDLVL2. There are many settings available through these system values. IBM provides some general values like *SECURITY, but you can add to this basic set by using the other system value options.

Enabling all of the auditing options will result in a VERY large number of events generated in the QAUDJRN journal. It is not uncommon to find several million events generated on a daily basis when all of these options are enabled. By default, Alliance LogAgent will process all of these events and transmit them to your log collection server.

Use the Work With System Values (WRKSYSVAL) command and review the settings in QAUDLVL and QAUDLVL2. Enable only the events you need for security event reporting. Consider turning off print management events and object access event logging. These can produce a very large number of events.

SECURITY NOTE: Be sure to check with your security administrator before changing any system values related to event collection to ensure that you are meeting all compliance regulations related to log collection.

Object Auditing

In addition to the system values that affect the types of events that are collected, you can also enable object level auditing using the Change Object Auditing (CHGOBJAUD) command. This command is used to enable or disable object level access auditing for programs, files, and almost any other type of object in your user libraries. If you enable object level auditing for an entire library, you may create a VERY large number of events in the QAUDJRN journal.

Consider using object level auditing on only the files and programs that are sensitive in nature. This can reduce the number of events and the amount of work that Alliance LogAgent needs to do for event reporting.

Filtering Events

Alliance LogAgent has the ability to filter events based on the security event type. You may be collecting a large number of events, but may not need to report all of these events to your log collection server. You can turn off the processing and transmission of selected events. From the main menu SYMAIN take option 2 for Configuration, then option 3 to Work With Security Types. Place a 2 next to a security type to change it. You will find the option to report the event on the first panel:

```
Send to log server . . . . . .    1        1=Yes, 2=No
```

You can change this option to 2 (No) to suppress processing this security event. This action takes effect immediately. This option does NOT change any system values or security options. Events will still be collected in the QAUDJRN journal, but will not be processed by Alliance LogAgent.

Application Logging

Alliance LogAgent provides for diagnostic logging to help you and the software support team quickly analyze potential problems. These diagnostic logging options cause the LogAgent to write data to log files in the product library. Application logging can have a negative impact on performance, and should only be enabled when you are trying to diagnose problems.

Communications Logging

The communications applications have an option for application logging. From the main menu SYMAIN take option 2 for configuration, then option 2 to Work With TCP Clients. Place a “2” next to your communications configuration. On the first panel you will find this option:

```
Application logging . . . . . .    2        1=Yes, 2=No
```

Be sure this option is set to 2 (No). If it is set to 1 (Yes), change it to 2 and update the configuration. Stop the ALLSYL100 subsystem and restart it. You can now clear the logging file ALLOGA:

```
clrpfm file(allsyl100/alloga)
```

Application Logging

The various collectors for the QAUDJRN security journal, QHST system message file, and QSYSOPR message queue can produce diagnostic information. From

the main menu SYMAIN take option 2 for Configuration, then option 1 to Configure Alliance LogAgent. On the first panel you will find this option:

Enable diagnostic logging . . . .2 1=Yes, 2=No

Make sure this option is set to 2 (No). If it is set to 1 (Yes), change it to 2 and update the configuration. End the ALLSYL100 subsystem and restart it.

Job Logging

If the Alliance LogAgent application is producing large job logs, you can reset the application to create basic job logs with the SYLOGOFF program:

call pgm(allsyl100/sylogoff)

This application will change all Alliance LogAgent job descriptions to use minimal logging.

Performance Architecture

Application Architecture

Alliance LogAgent is designed to work the way any normal IBM I application would work. The application does not make any changes to the system to allocate CPU or disk resources, and does not system API calls to manipulate resources. It is designed to behave in the way any user application would work on the IBM I. This means that you can easily manage the resources used by Alliance LogAgent.

Journal Event Processing

To maximize performance and minimize the impact on your system, Alliance LogAgent retrieves a large block of security events each time it accesses the QAUDJRN journal entries. The process of reading events from the journal is expensive on CPU resources, so Alliance LogAgent attempts to minimize this impact by reading many events at one time. This also improves the ability of Alliance LogAgent to handle many events per second.

While Alliance LogAgent retrieves many entries from the journal at a time, it only processes one event at a time. An event is converted to syslog format, queued for transmission, and sent to your log collection server before the next event is processed. This means that the application will naturally give up resources to other active applications, and will not “capture” CPU resources through intensive CPU activity.

Subsystem Architecture

The Alliance LogAgent jobs run in a subsystem named ALLSYL100. All of the jobs run at a priority of 50 which is a batch priority level. Even when Alliance LogAgent is processing a large volume of events it will not affect interactive performance. Of course, if your IBM i is already over-committed on CPU or disk resources, Alliance LogAgent may affect overall system performance. This would be true for any new application you installed on your system.

Job Priorities and Time Slice

Because Alliance LogAgent runs at a batch priority of 60, it may affect the performance of other batch jobs running at the same priority. The i5/OS operating system will attempt to balance resources between multiple jobs running at this priority. You can lower the priority of the Alliance LogAgent jobs by changing the class ALLSYL100. For example, you can change the priority to 70 using this command:

chgcls cls(allsyl100/allsyl100) runpty(70)

Note that changing the priority to a very low level may cause the application to report events some time after they occur. Managing the priority of the Alliance LogAgent involves balancing your needs for timely information and your need for system performance.

The Alliance LogAgent application is configured to use a timeslice of 2000 in the batch environment. This should ensure that Alliance LogAgent share resources with other applications on the system. However, in some environments you may have better performance by increasing or decreasing this value. Discuss this value with your system administrator. You can change the value using the Change Class (CHGCLS) command:

chgcls cls(allsyl100/allsyl100) timeslice(5000)

IMPORTANT: If you change the subsystem or class provided in the Alliance LogAgent library, you must remember to re-apply these changes after you upgrade the product.

CPU Utilization

High CPU Utilization On A New Installation

If you just installed Alliance LogAgent and you observe that it runs continually and registers high CPU utilization, it may be because Alliance LogAgent is processing historical events. By default, Alliance LogAgent will begin processing the oldest available events in the QAUDJRN security journal. If you have several weeks or months of data in the

QAUDJRN it may take some time for Alliance LogAgent to process all of these events. Eventually Alliance LogAgent will finish processing the historical data and reduce its use of system resources.

NOTE: You can set the starting point for log collection using option 7 (Change QAUDJRN Starting Point) on the configuration menu. You can set the starting point to a specify journal receiver, or to a specific date and time. This can greatly reduce the amount of processing needed for a new installation.

High CPU Utilization During Normal Operation

During normal processing you may see high CPU utilization rates by the Alliance LogAgent jobs. It is not uncommon to observe CPU utilization rates of 25 percent or higher. While the Alliance LogAgent jobs run at a low priority, the i5/OS operating system will give the application CPU resources if they are available. This is a normal condition and you should not observe a negative impact on interactive user jobs. Temporary high CPU utilization may indicate that Alliance LogAgent is "catching up" by processing past events, or system activity generated a lot of events to process (see the section above about configuring system values).

Spikes In Utilization

If you notice spikes in CPU utilization it almost always due to a spike in the number of QAUDJRN events that are being generated by the i5/OS operating system. This could be caused by a nightly backup, or other activity that affects a large number of objects in user libraries. Review your system logs to determine what types of events are being collected during the time you observe the spike in activity. Look especially for ZR (object access) events and AD (authority adoption) events. You may want to adjust your security values to better manage the types of events that are being generated and processed by Alliance LogAgent.

Disk Utilization

Capturing Events To A Physical File

Alliance LogAgent does not collect events in disk files even when processing a high volume of security events. This means that normal use of Alliance LogAgent should not have a significant impact on disk utilization. However, Alliance LogAgent gives you the ability to capture events to a user-defined file on your IBM I. Because event information can be quite large, and because there can be a very large number of events, this file can become quite large. Use option 1 (Configure Alliance LogAgent) to view the file collection option:

```
Capturetologfile .....2     1=Yes,2=No
File / Library / Member . . . .SYLOGF ALLSYL100 SYLOGF
```

If the option is enabled you may want to turn it off and clear any captured events.

Application Logging

As mentioned above, Alliance LogAgent provides options for collecting application events for diagnostic logging. If you observe the file ALLOGA in the ALLSYL100 library becoming large, you should turn off the communications logging option (see above). You can then clear the file:

```
clrpfm file(allsyl100/alloga)
```

Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, Linux, and UNIX. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.